ABSTRACT

METHOD FOR MIGRATING A BASE CHIP KEY FROM ONE COMPUTER SYSTEM TO ANOTHER

A method for migrating a base chip key from a first computer system to a second computer system is disclosed. A first computer system includes a base chip key 1, and a second computer system includes a base chip key 2. Using a first certificate for the base chip key 1, a manufacturer of the second computer system generates a second certificate for the base chip key 1. Similarly, using a first certificate for the base chip key 2, a manufacturer of the first computer system generates a second certificate for the base chip key 2. A first data packet is then sent from the first computer system to the second computer system. The first data packet includes a first random number and all the data required to reproduce the base chip key 1 in the first computer system. The first data packet is also encrypted with the base chip key 1's public key. In return, a second data packet is sent from the second computer system to the first computer system, and the second data packet includes the first random number and a second random number, signed by the base chip key 2. The base chip key 1 is then erased from the first computer system. Finally, the base chip key 2 in the second computer system is replaced by the base chip key 1.